AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A processor comprising:

a plurality of pipeline stages to perform an inner loop of a hash algorithm, the plurality of pipeline stages comprising at least as many pipeline stages as there are iterations of the inner loop to be performed, wherein each iteration of the inner loop is performed by a dedicated pipeline stage.

2. (Original) The processor of claim 1 wherein the plurality of pipeline stages further comprises as many pipeline stages as there are chaining variables to be used in the inner loop.

3. (Original) The processor of claim 2 wherein each pipeline stage comprises an adder, a shifter, and logic to perform a function.

4. (Original) The processor of claim 3 further comprising control logic to schedule operations to be executed within the plurality of pipeline stages.

5. (Original) The processor of claim 4 wherein operations are to be scheduled by the control logic and executed by the plurality of pipeline stages so as to minimize data dependencies between iterations of the inner loop to be performed.

6. (Original) The processor of claim 5 wherein the hash algorithm is chosen from a

group of secure hash algorithms (SHA) consisting of SHA-1, SHA-128, SHA-196, SHA-256, and message digest 5 (MD5).

7. (Original) The processor of claim 6 wherein the hash algorithm is to be performed at an operating frequency equal to that of the adder.

8. (Original) The processor of claim 7 wherein the plurality of pipeline stages comprises 88 pipeline stages to process 512 bits of data.

9. (Original) An apparatus comprising:

a first plurality of pipeline stages to perform a hash including:

a first pipeline stage to add a first constant to a first data word to yield a first result;

a second pipeline stage to add the first result a first chaining variable, perform a first function on a second, third, and fourth chaining variable to yield a second result, and add the first constant to a second data word to yield a third result;

a third pipeline stage to add the second result to the sum of a fifth chaining variable and the first result, add the first constant to a third data word, add the third result to the fourth chaining variable, perform the first function on the first, second, and third chaining variables after they each of have been shifted by a plurality of bits;

a second plurality of pipeline stages to add an initial state of the first, second, third, fourth, and fifth chaining variables to a final state of the first, second, third, fourth, and fifth chaining variables, respectively.

10. (Original) The apparatus of claim 9 wherein the first plurality of pipeline stages comprises 83 pipeline stages to process 512 bits of information.

11. (Original) The apparatus of claim 9 wherein the second plurality of pipeline stages comprises 5 pipeline stages to process 512 bits of information.

12. (Original) The apparatus of claim 9 wherein the first and second plurality of pipeline stages are implemented within a network processor architecture.

13. (Original) The apparatus of claim 9 wherein the hash algorithm is a secure hash algorithm (SHA) and the plurality bits is 30.

14. (Original) The apparatus of claim 9 wherein the network processor architecture is to perform the hash algorithm at an operating frequency of at least 1.4 GHz.

15. (Original) A machine-readable medium having stored thereon a set of instructions, which if executed by a machine cause the machine to perform a method comprising:

performing a plurality of iterations of an inner loop of an hash algorithm in parallel, the plurality of iterations performed in parallel being limited, at least in part, by dependencies between each of the plurality of iterations of the inner loop;

adding initial values of a plurality of chaining variables to final values of the

plurality of chaining variables, the final values being a result of performing the plurality of iterations of the inner loop.

16. (Previously Presented) The machine-readable medium of claim 15 wherein the method further comprises controlling scheduling of operations performed as a result of performing the plurality of iterations of the inner loop, the scheduling being controlled so as to minimize a critical path among the operations.

17. (Original) The machine-readable medium of claim 16 wherein the critical path depends upon the dependencies between the plurality of iterations of the inner loop.

18. (Original) The machine-readable medium of claim 17 wherein the method further comprises decoding the inner loop of the hash algorithm into a first number of operational stages, the first number of operational stages being equal to at least the plurality of iterations.

19. (Original) The machine-readable medium of claim 18 wherein the inner loop is to be performed to process a first number of data elements transmitted over a network.

20. (Original) The machine-readable medium of claim 19 wherein the first number of operational stages is at least 83 and the first number of data elements comprises 512 bits.

21. (Original) A method comprising:

performing a hash algorithm within a pipelined processor by performing a plurality of iterations of an inner loop of the hash algorithm in parallel;

generating a plurality of output data elements as a result of performing the hash algorithm.

22. (Original) The method of claim 21 further comprising scheduling operations associated with the plurality of iterations so as to facilitate a maximum number of the operations to be performed in parallel.

23. (Original) The method of claim 22 wherein the maximum number depends upon dependencies between the operations.

24. (Original) The method of claim 22 wherein the output data elements are transmitted within a computer network.

25. (Previously Presented) The method of claim 24 wherein the hash algorithm is performed at the operating frequency of the processor.

26. (Previously Presented) The method of claim 25 wherein the hash algorithm is performed at 1.4 GHz.

27. (Original) A system comprising:

a memory unit to store operations of a hash algorithm;

a pipelined processor to perform the operations of the hash algorithm by performing iterations of an inner loop of the hash algorithm within separate pipeline stages of the pipelined processor.

28. (Original) The system of claim 27 wherein the operations are scheduled so as to minimize the number dependencies among the operations.

29. (Original) The system of claim 28 further comprising a bus upon which to drive data generated by performing the hash algorithm within the pipelined processor.

30. (Original) The system of claim 28 further comprising a bus to receive data to be operated on by the pipelined processor to perform the hash algorithm.

31. (Original) The system of claim 30 wherein 512 bits of data is to be processed by at least 83 pipeline stages of the pipelined processor.

32. (Original) The system of claim 27 wherein the pipelined processor is a network processor coupled to a network.

33. (Original) The system of claim 32 further comprising a host processor coupled to the network processor to perform a portion of the hash algorithm.

34. (Original) The system of claim 27 wherein the hash algorithm is chosen from a

group of secure hash algorithms (SHA) consisting of SHA-1, SHA-128, SHA-196, SHA-256, and message digest 5 (MD5).

35. (Original) An apparatus comprising:

execution means for performing iterations of an inner loop of a hash algorithm in parallel including:

first means for adding a first constant to a first data word to yield a first result;

second means for adding the first result a first chaining variable, performing a first function on a second, third, and fourth chaining variable to yield a second result, and adding the first constant to a second data word to yield a third result;

third means for adding the second result to the sum of a fifth chaining variable and the first result, adding the first constant to a third data word, adding the third result to the fourth chaining variable, performing the first function on the first, second, and third chaining variables after they each of have been shifted by a plurality of bits;

adding means for adding an initial state of the first, second, third, fourth, and fifth chaining variables to a final state of the first, second, third, fourth, and fifth chaining variables, respectively;

scheduling means for scheduling operations associated with the hash algorithm.

36. (Original) The apparatus of claim 35 wherein the execution means is a pipelined architecture and wherein each of the first, second, and third means are pipeline stages of the pipelined architecture.

37. (Original) The apparatus of claim 35 wherein the scheduling means is a controller to schedule operations associated with the inner loop according to dependencies among the operations.

38. (Original) The apparatus of claim 36 wherein each iteration of the inner loop requires three pipeline stages to perform the iteration.

39. (Original) The apparatus of claim 38 wherein the adding means comprises the same number of pipeline stages as chaining variables.

40. (Original) The apparatus of claim 35 wherein the hash algorithm is chosen from a group of secure hash algorithms (SHA) consisting of SHA-1, SHA-128, SHA-196, SHA-256, and message digest 5 (MD5).

41. (Original) The apparatus of claim 35 wherein the plurality of bits is 30.